بزهکاری پیشرفته (بخش دوم)

جرایم رایانه‌ای و اینترنتی (قسمت اول)

محمد اسحاقی

چکیده:

«انقلاب و انفجار اطلاعات» نامی است که بر دهه آخر قرن بیستم نهاده شده است.

پیشرفت فن‌آوری در سده اخیر سبب بروز انقلابهایی در زندگی بشر امروز شده و این پیشرفتها در واپسین دهه‌های قرن بیستم رشد و سرعت فزاینده‌ای گرفته است؛ به گونه‌ای که به اعتقاد بعضی یک گسستگی تاریخی در سیر پیشرفت دانش بشر مشاهده می‌شود. این بار بشر با انقلابی دیگر روبه‌روست؛ انقلاب و انفجار اطلاعات و به همین سبب عصر کنونی را عصر اطلاعات نامیده‌اند.

در این میان فن‌آوری اطلاع رسانی از یک طرف و افزایش اطلاعات به وسیله بهره‌مندی از وسایل اطلاع رسانی پیشرفته از طرف دیگر، همانند یک واکنش دو طرفه تأثیر متقابل داشته و افزایش تصاعدی اطلاعات و پیشرفت فن‌آوری اطلاع‌رسانی را در پی آورده است. همچنین تسهیلات ایجاد شده جهت استفاده از بزرگراههای اطلاعاتی و اتصال به آن بر ویژگی آن افزوده است؛ در دو تحلیل کاملاً متضاد - یکی کاملاً خوشبینانه و دیگری کاملاً بدبینانه - این شبکه‌ها تنها برای توسعه و تحول عملی و یا برای حاکمیت و تسلط بر فرهنگ کشورها و تخریب بافت سالم جوامع تحت سلطه شبکه‌های اطلاع‌رسانی به وجودآمده و هر روز در حال توسعه است.

نقش سازنده شبکه‌های اطلاع رسانی در توسعه و ضرورت استفاده و اتصال به آن از یک طرف و نیز نقش مخرب آن در زوال فرهنگها و توسعه بزهکاری پیشرفته و تسهیل آن از طرف دیگر، ما را بر آن می‌دارد که با دقت بیشتر و هرچه سریعتر به دنبال راهکارهای اجرایی استفاده صحیح از شبکه‌های اطلاع رسانی در کشور، ایجاد فرهنگ استفاده سازنده و جلوگیری از سوء استفاده از آن باشیم.

مقدمه:

◄ در شماره گذشته به مبانی نظری «بزهکاری پیشرفته» اشاره شد. آنچه در این میان اهمیت دو چندان می‌یابد، این حقیقت است که همگام با سیر فزاینده رشد و توسعه «فن‌آوری» و تأثیر مستقیم آن بر تنوع، تکثر و پیچیدگی «بزهکاری»، باید نمودهای عینی و قابل تجربه نیز مورد مطالعه قرار گیرد و مسؤولان مبارزه با بزهکاری با نمونه‌های عینی «بزهکاری پیشرفته» آشنا شده و در مراحل بعدی امکان مقابله با آن را در خود فراهم نمایند.

این یک واقعیت گریزناپذیر است که بزهکاری در حال پیشرفت می‌باشد و ما هر روز با گونه‌های جدید آن آشنا می‌شویم. به همین خاطر لازم است بطور دقیق انواع و شکلهای گوناگون آن شناسایی و ماهیت هر یک و نحوه عمل بزهکاران و چگونگی مقابله با آن کشف شود و در جهت مقابله با آن، اقدامات لازم صورت گیرد که به همین سبب، این نوشتار در صدد معرفی مصادیق بزهکاری پیشرفته و نوع عمل بزهکاران است. باید گفت بعضی از فن‌آوریهای پیشرفته به خاطر ماهیت خود، نقش و توانایی زیادی در وقوع و ایجاد بزهکاری از خود نشان داده‌اند و اقدام بزهکارانه را برای همگان سهل و آسان نموده‌اند و

در مقابل، بعضی از فن‌آوریهای پیشرفته به خاطر طبیعت و ماهیت خود، که بیشتر جنبه تخصصی دارند، کمتر مورد استفاده عمومی بزهکاران قرار می‌گیرند. بنابراین، در اولین گام در شناسایی مصادیق و نمونه‌های عینی «بزهکاری پیشرفته»، به عالم پر رمز و راز و به ظاهر لایتناهی شبکه‌های اطلاعاتی و رایانه‌ها بخصوص «*اینترنت*» گام می‌گذاریم و نحوه عمل بزهکاران را در این وادی به نظاره می‌نشینیم.

در آغاز برای جلوگیری از هرگونه سوءبرداشت، پیشداوری و خروج از دایره حق ضمن تعریف و بیان سابقه شبکه‌های رایانه‌ای، به «طرف روشن شبکه‌های اطلاع رسانی» و مزایای فراوان و منحصر به فرد «شبکه‌های رایانه‌ای» یا «*اینترنت*»، که لزوم استفاده از آن را برای انسان کنونی (حتی در زندگی معمولی خود) به شکل امری گریزناپذیر درآورده اشاره می‌کنیم. سپس به موضوع اصلی این شماره که همانا «بزهکاری رایانه‌ای و اینترنتی» باشد، باز می‌گردیم؛ به عبارت دیگر به «طرف تاریک شبکه‌های اطلاع رسانی» نیز اشاره خواهیم کرد.

تعریف اینترنت

اینترنت یک شبکه گسترده بین‌المللی و از شبکه‌هایی است که به هر نوع رایانه‌ای امکان می‌دهد تا در خدمات آن سهیم شود و مستقیماً ارتباط برقرار کند؛ به گونه‌ای که این رایانه‌ها جزئی از یک دستگاه رایانه‌ای عظیم جهانی به شمار می‌روند. این شبکه که از گسترده‌ترین شبکه‌های جهانی است، علاوه بر رایانه‌های مستقل و شبکه‌های کوچک محلی، بیشتر شبکه‌های جهانی را نیز در دل خود جای داده و امکان تبادل اطلاعات را بین آنها فراهم نموده است. لذا ***اینترنت*** را «مادر شبکه‌ها» می‌نامند.

سابقه

سال ۱۹۶۹: سابقه راه‌اندازی ***اینترنت*** به شبکه دیگری به نام «آرپانت» بر می‌گردد که در سال ۱۹۶۹ میلادی توسط آژانس طرحهای تحقیقاتی پیشرفته در وزارت دفاع آمریکا راه اندازی شد. این شبکه دسترسی رایانه‌ها را از راه دور به مرکز رایانه میسر می‌ساخت.

سال ۱۹۸۰: شبکه «***اینترنت***» در شکل اولیه خود با هدف متصل کردن شبکه‌های جهانی با قراردادهای ارتباطی متفاوت با یکدیگر به وجود آمد.

سال ۱۹۸۳: بخش نظامی شبکه «آرپانت» از آن جدا شد و تحت شبکه «میل‌نت» آغاز به کار کرد.

سال ۱۹۹۰: دراین‌سال،شبکه«آرپانت»کاملاًجای‌خودرا به «***اینترنت***» داد.

اکنون در سال ۲۰۰۰ میلادی هستیم. از آن سال تاکنون این شبکه با سرعت چشمگیری از جهت تعداد استفاده‌کنندگان و حجم تبادل اطلاعات، در حال گسترش است وهم اکنون برخی از رایانه‌ها، در قریب به اتفاق کشورهای جهان به ***اینترنت*** متصل می‌باشند. تخمین زده می‌شود متجاوز از ۲۰۰ میلیون نفر از ***اینترنت*** استفاده می‌کنند که این رقم به سرعت در حال افزایش است؛ به طور نمونه هر ۵۳ روز یک بار، حجم تبادل اطلاعات ۲ برابر می‌شود.

خدمات شبکه

خدمات و توانایی‌های شبکه اینترنت به سرعت در حال افزایش و تخصصی‌شدن‌است‌که‌درزیر،مهمترین خدمات عمومی این شبکه بیان می‌شود.

۱- **پست الکترونیک**: در این سرویس متن یا هر پرونده رایانه‌ای دیگری توسط یک دستور و معمولاً ظرف چند ثانیه به هر نقطه‌ای از دنیا و به هر نوع رایانه ارسال می‌شود.

۲- **سرویس دسترسی به اطلاعات**: اطلاعات زیادی در شبکه‌های

رایانه‌ای است که می‌توان از طریق «**اینترنت**»، به آنها دست یافت. این اطلاعات می‌تواند به صورت متن، صوت، تصویر و یا حتی فیلم باشد. جهت سهولت در آماده سازی و بازیابی این اطلاعات در شبکه ***اینترنت*** از روشهای استاندارد شده‌ای مانند Gopher و world wide (W W W) استفاده می‌شود.

۳ـ سرویس انتقال پرونده‌های رایانه‌ای: تعداد زیادی رایانه در شبکه ***اینترنت*** وجود دارند که بر روی آنها، پرونده‌های رایانه‌ای شامل برنامه، متن و...جهت استفادهٔ اعضای شبکهٔ ***اینترنت*** قرار داده شده است. برای انتقال این پرونده‌ها به رایانه شخصی استفاده‌کنندگان، می‌توان از سرویس انتقال پرونده‌های رایانه‌ای استفاده نمود.

۴ـ سرویس گروههای تخصصی: گروههای تخصصی متنوعی می‌توانند بر روی شبکه ایجاد شود. هم اکنون هزاران گروه تخصصی روی ***اینترنت*** موجود است که در حیطه وسیعی، از علاقه‌مندان به جمع‌آوری تمبر تا گروه متخصصان فیزیک هسته‌ای را در برمی‌گیرد. در این گروهها، هر اطلاعاتی که رد و بدل گردد، برای تمامی اعضا فرستاده می‌شود و اعضای گروه در دورترین نقاط جهان به آخرین دستاوردها در زمینه‌های مورد علاقه خود دسترسی یافته و نیز یافته‌های خود را به دیگر علاقه‌مندان منتقل می‌کنند.

۵ـ سرویس کنفرانس الکترونیکی: توسط این سرویس می‌توان کنفرانسهای از راه دور، بین دو یا چند نفر برقرار نمود. هم اکنون در شبکهٔ ***اینترنت*** علاوه بر برقراری کنفرانسها با استفاده از تایپ متن، امکان استفاده از صدا و تصویر شرکت کنندگان نیز وجود دارد.

۶ـ سرویس دسترسی به رایانه از راه دور: به وسیله این سرویس هر عضو قادر است تا از هر رایانه در گوشه جهان جهت انجام عملیات مورد نظر خود استفاده کند.

۷ـ سرویس خبری: هم اکنون بیش از ۱۵۰ مجله و روزنامه الکترونیکی

(بسیاری از روزنامه‌ها، مجلات داخلی و خارجی، شبکه‌های رادیو تلویزیون محلی و ماهواره‌ای به زبان فارسی و غیر آن) بر روی شبکه *اینترنت* منتشر می‌شود که دسترسی به آخرین اخبار و رویدادها را برای اعضا ممکن می‌کند.

طرف تاریک شبکه‌های اطلاع رسانی

در کنار کاربردهای متنوع شبکه‌های اطلاع رسانی، توجه به طرف تاریک آن درکشورهای دارای فرهنگ محوری از اهمیت بسزایی برخوردار است. کاربردهای سوء از این فن‌آوری نوین، یک نگرانی در سطح جهان پدید آورده است؛ به گونه‌ای که هم اکنون هیچ کشوری را در شرق و غرب جهان نمی‌توان یافت که نسبت به سوءاستفاده از آن ابراز نگرانی نکرده باشد. آمارهای منتشر شده نشان می‌دهد روزانه بیش از ۱۰۰ میلیون نفر به گشت و گذار در جهان اطلاعات مشغولند.

شبکه‌های اطلاع رسانی مانند یک جهان واقعی و (البته در بعدی دیگر) نقش بازی می‌کند. در این جهان افراد بداندیش، بیماران روانی، بزهکاران با سابقه و... دیگری نیز وجود دارند که از «شبکه‌های اطلاع رسانی» برای انجام کارهای خلاف خود استفاده می‌کنند. سوء استفاده از *اینترنت* در محورهای مختلف انجام می‌گیرد و هر روز بر تنوع و گستردگی آن افزوده می‌شود که در اینجا به نمونه‌هایی از عملکرد بزهکارانه شبکه‌های اطلاع رسانی جهانی (*اینترنت*) اشاره می‌کنیم:

مخابره مطالب و تصاویر جنسی وقیحانه و نمایش صحنه‌های خارج از نزاکت

یکی از اقلام موجود در شبکه‌های اطلاع‌رسانی، مطالب، عکسها، فیلمها و پیامهای فسادانگیز است. از هر ده کلمه‌ای که روی *اینترنت* جست و جو می‌شود؛ یعنی کلماتی که افراد با استفاده از رایانه تایپ می‌کنند تا اطلاعات

معینی را کسب کنند، شش کلمه راجع به مطالب هرزه است.

بررسی ای که اخیراً توسط مجله "Web" به عمل آمده، نشان می‌دهد که حتی برای منحرفترین کاربران *اینترنت* هم میزان علاقه به سکس در این شبکه شاید حیرت‌انگیز باشد. طی یک دوره یک ماهه معلوم شد که کلمه «سکس» محبوبترین کلمه کاربران شبکه است و در این مدت، بیش از یک میلیون بار، این کلمه تایپ شده و مورد جست و جو قرار گرفته است. دومین کلمه مورد علاقه «گپ» بوده کاربران که ۷۵ درصد کمتر به آن علاقه نشان داده شده است.

فهرست کامل ده کلمه مورد علاقه استفاده‌کنندگان شبکه به ترتیب اهمیت عبارت است از: ۱ـ سکس، ۲ـ گپ، ۳ـ XXX، ۴ـ پلی بوی، ۵ ـ نرم‌افزار نت اسکیپ، ۶ـ لخت، ۷ـ پورنو، ۸ـ بازی، ۹ـ هوا، ۱۰ـ نپت هاوس. دهها کلمه دیگر نیز در ارتباط با سکس هست که تعداد آنها به دویست می‌رسد.(۱۰)

بسیاری از رسانه‌های جهان غرب، بویژه آمریکا، کارکنان خود را در ساعات کار از مشاهدهٔ عکسها و فیلمهای مستهجن و گپ زدن با دخترها و پسرها به وسیله *اینترنت* از طریق ارسال پیام و نیز خواندن مراکز فساد و زنان و مردان ولگرد و... منع کرده‌اند.

انتشار عکسهای ضد اخلاقی کودکان از جمله موارد موجود در *اینترنت* است. در *اینترنت* نیز همانند جهان واقعی گروهی به اغفال کودکان می‌پردازند. یکی از این موارد در ایالت کنتاکی در آمریکا اتفاق افتاد. در آنجا یک بازرس پلیس موفق شد یک شبکه انتشار عکسهای ضد اخلاقی کودکان را از بین ببرد.(۲)

در آمریکا نخستین واکنشها علیه «*اینترنت*» در مخالفت با اینگونه خدمات بوده است. یک زوج جوان آمریکایی اقدام به ایجاد یک خبرنامهٔ سکسی کردند که بینندگان زیادی در سراسر جهان داشت و از این طریق درآمد

سرشاری به دست آوردند.

یکی از جدیدترین نمونه‌های بدآموز و زننده *اینترنت* از این قرار است:

یک دختر و پسر آمریکایی ۱۸ ساله به نامهای «دایان» و «مایک» که خود را زن و شوهر می‌نامیدند، چندی پیش در شهر لس‌آنجلس اعلام کردند که روز معینی که آن هم اعلام شد، با هم عروسی خواهند کرد و مراسم حجله که مجهز به دوربین فیلمبرداری است، از طریق یک «وب سایت Web Site» که برای خود در *اینترنت* ساخته‌اند، مستقیماً در سراسر جهان پخش خواهد شد. این زننده‌ترین کاری بود که تاکنون از طریق *اینترنت* به عمل آمده است. گفتنی است هم اکنون راهی برای پیشگیری از انتشار و دستیابی به مطالب خلاف عفت عمومی وجود ندارد و تلاشهای متخصصان امر تاکنون نتیجه بخش نبوده است؛ به گونه‌ای که شرکتهای مؤتلفه اطلاع رسانی از طریق *اینترنت*، طی اطلاعیه‌ای بر مراتب عجز خود در پیشگیری از انتشار مطالب «ناخواسته» در *اینترنت* تأکید کرد ه‌اند. دولت آمریکا و دولتهای دیگر از جمله آلمان از این شرکتها خواسته بودند که مانع از قرارگرفتن مطالب، عکسها، فیلمها و پیامهای فسادانگیز در *اینترنت* شوند.

تعداد بینندگان این برنامه‌ها بیشتر از نود درصد هستند و متقاضیان اطلاعات مفید، در حال حاضر کمتر از ۹ درصدند و بدین ترتیب شبکه‌های اطلاع رسانی خصوصاً *اینترنت* بزودی نقش «بزرگترین بدآموز بین‌المللی» را پیدا خواهد کرد. عمق فاجعه آنگاه آشکار می‌شود که پای کودکان به عنوان کاربر و استفاده کننده از شبکه به میان بیاید.

بزهکاری انفورماتیک

امروزه و یا در آینده نه چندان دور، اکثر نقل و انتقالهای پولی و مالی در بازار اقتصاد از طریق رایانه انجام می‌پذیرد. امر تولید در

بسیاری از شرکتها به مغز الکترونیکی وابسته است و بسیاری از مؤسسات تجاری، اطلاعات سرّی مربوط به معاملات و فعالیتهای بازرگانی را در رایانه انبار می‌کنند. همینطور ادارات با سیستمهای جدید انفورماتیک کار می‌کنند. این موضوع در مورد روشهای مراقبت هوایی، ناوبری هوایی، و کنترل رفت و آمد کشتیها و سیستمهای کنترل امور پزشکی نیز صادق است. نتیجه اینکه توسعه داده‌های رایانه‌ای در بانک، تجارت و صنعت می‌تواند موجب ترس از قریب‌الوقوع بودن استفاده از روشهای اجرایی از سوی بزهکاران متخصص شود.

با تولد رایانه‌ها ملاحظه می‌شود که نوع جدیدی از جرایم مرتبط به آن در روبه‌روی جرم‌شناسان و نیروهای امنیتی قرار گرفته است. بزهکاری انفورماتیک روز به روز متنوع شده و اکنون اشکال شناخته شده‌ای همچون خرابکاری، جاسوسی، سرقت، استفاده و دستکاری غیرقانونی در رایانه‌ها و... را شامل می‌شود. در دهه ۱۹۷۰ میلادی، نخستین پژوهشهای علمی و جرم شناختی در این زمینه انجام شد و بدین ترتیب از یک سو به اشکال متعددی از بزهکاری انفورماتیک و از سوی دیگر به رقم سیاه قابل توجه در این نوع بزهکاری، پی برده شد.

به عنوان نمونه فهرست اعمال مجرمانه در قلمرو انفورماتیک و رایانه که بوسیله شورای اروپا تهیه و معرفی شده به این شرح است؛ تقلب نسبت به رایانه، تقلب نسبت به انفورماتیک، وارد کردن خسارت به داده‌ها یا برنامه‌های انفورماتیک، خرابکاری و دستکاری غیرقانونی در رایانه، ورود غیرمجاز به سیستمها و داده‌های انفورماتیک، رهگیری غیرمجاز ارتباطات رایانه‌ها، تولید غیرمجاز برنامه رایانه و انفورماتیک حمایت شده، تکثیر غیرمجاز یک توپولوژی، جاسوسی با رایانه و استفاده غیرمجاز از یک رایانه.[۳]

موارد سرقت داده‌ها و اطلاعات رایانه‌ای و سوءاستفاده از سیستمهای رایانه‌ای در زمینه ارتباطات یعنی پدیده مشهور هکینگ Hacking که باعث آسیب‌پذیر شدن مؤسسات مختلف صنعتی، بانکی، بازرگانی و دولتی می‌گردد، هر روز در حال افزایش است.

امروزه در زمینه جرایم رایانه‌ای و انفورماتیک، عمدتاً پدیده هکینگ، مسأله دستکاری غیرقانونی در سیستمهای نقل و انتقال الکترونیکی سرمایه‌ها مشاهده می‌شود. خطر این پدیده برای نخستین بار در سال ۱۹۸۹، زمانی برای عموم آشکار شد که در دادگستری آلمان، دادرسی کیفری علیه چند آلمانی در جریان بود که از طریق شبکه‌های انفورماتیک بین‌المللی در سیستمهای انفورماتیک آمریکا، انگلستان و سایر کشورهای خارجی نفوذ کرده بودند و اطلاعات به دست آمده از این طریق را به سرویسهای مخفی شوروی سابق، یعنی K.G.B فروخته بودند.

اینترنت - ورم (Internet-Worm)، متعلق به یک دانشجوی آمریکایی در همان سال، موفق شده بود شش هزار رایانه «*اینترنت* - سیستم» (Internet-System) را به مدت چند روز فلج کرده و از کار بیندازد.(۴)

همچنانکه ملاحظه شد، ارتکاب این نوع از بزهکاری، مستلزم مداخله متخصص می‌باشد و به طور کلی این برنامه‌ریز است که در برنامه‌های رایانه‌ای مربوط به حسابها، مثلاً دستور انتقال مبلغی را به حسابی که قبلاً باز شده است، وارد می‌کند. یکی از این متخصصان، که کارمند بانک بود، انتقال اعتبار ده میلیون دلاری را برنامه‌ریزی کرده بود. گاه اختلال مزبور متقلبانه‌تر است؛ مثلاً مورد معروف یک متخصص داده‌های رایانه‌ای برنامه‌ریزی کرد که تمام اعداد «صد» را که در عملیات ظاهر

می‌شد، به حسابی که خود بازکرده بود، واریز گردد. و به این ترتیب حسابها را «سرراست» نموده بود. با این روش وی موفق به جمع کردن مبلغ قابل توجهی شد و فقط به کمک ادعاهای یک مشتری دقیق مبنی بر اینکه در حساب او بیش از ۷۰ دلار زلاندنو نیست، در صورتی که موجودی این حساب قبلاً بالغ بر ۷۱ دلار زلاندنو بوده است، کشف می‌شود.(۵)

عدم وجود امنیت در شبکه‌های اطلاع رسانی

بسیاری از متخصصان امور شبکه‌های اطلاع‌رسانی، بزرگترین مشکل این شبکه‌ها را مسأله امنیت می‌دانند. آنچه تاکنون در جهان مجازی شبکه‌های اطلاع رسانی اتفاق افتاده، ناامنی را به صورت باور نکردنی به نمایش گذاشته است. این ناامنی تمام زندگی فردی و اجتماعی را می‌تواند در بر بگیرد و به مدد پیشرفت فن‌آوری رایانه‌ای، بر وسعت این ناامنی بیش از پیش افزوده می‌شود. این ناامنی آنگاه بیشتر آشکار می‌گردد که بدانیم مراکز نظامی ابرقدرتی همانند ایالات متحده آمریکا نیز به راحتی مورد حمله قرار می‌گیرد و مهاجم به راحتی به اطلاعات مورد نیاز خود دست می‌یابد. هفته نامه Defence News (اخبار نظامی) می‌نویسد:

«یک راهزن کامپیوتری به مغز سیستم کامپیوتری مدرسه عالی نیروی دریایی مانتری (کالیفرنیا) دسترسی پیدا کرده است. این اقدام باعث هراس مقامات نظامی آمریکا شده است».

دیفنس نیوز می‌نویسد:

«در پی این واقعه مقامات نظامی و صنعتی آمریکا از این که ممکن است «اینترنت» به صورت یک کانال اطلاعاتی به بانک اطلاعات پنتاگون (وزارت دفاع آمریکا) راه

پیدا کند، دچار وحشت شده‌اند».[۱]

در این میان تسهیلات فراوان و روشهای ساده ابداعی بر دامنه این ناامنی و بر تعداد «بزهکاران رایانه‌ای» افزوده است. اگر چه بزهکاری رایانه‌ای عموماً از سوی متخصصان صورت می‌گیرد، ولی با ابداع روشهای جدید و ساده از سوی متخصصان و آموزش آن به افراد غیر متخصص، دیگر جای امنی را بر پهنه گسترده شبکه‌های اطلاع رسانی جهانی و حتی در فایلهای رایانه شخصی و خانگی نمی‌توان یافت!

حمله اینترنتی

امروزه انتشار و ارسال ویروسهای رایانه‌ای خطرناک به شبکه‌های جهانی و رایانه‌های شخصی، به صورت یک اقدام عادی و معمولی ولی در عین حال وحشتناک و ناامید کننده در آمده است. ظهور ویروسها، همانند حمله ناگهانی مهاجمان قدرتمند و بی‌رحم به ساکنان بی‌پناه یک آبادی در نیمه‌های شب می‌باشد. تصور این واقعیت که یک دانشمند و محقق در پی مشاهده یک پیام ناآشنا بر صفحه مونیتور خود، همه تحقیقات، مطالعات، توصیفات و یافته‌های خود را نابود شده ببیند و یا تصور اینکه صورت عام مبادلات و عملیاتهای بانکی رایانه‌ای یک بانک زنجیره‌ای، که دارای شعب متعدد در سراسر جهان است، با اقدام از سر عقده یا شوخی یک آدم ناراحت به صفحه‌ای سفید تبدیل شود و همچنین تصور نتایج به عمل آمده از طریق این اقدام در حوزه‌های دیگر، تخم بیم و ناامیدی را به نحو گسترده‌ای در سراسر جهان می‌پراکند.

به عنوان نمونه یکی از ویروسهایی که در گذشته‌ای نه چندان دور به

۱- رسانه سال ششم، بشماره ۴، ص ۴۹.

سایتهای رایانه‌ای حمله نمود، برنامه‌ای است که می‌تواند حتی ناشی‌ترین افراد را در صحنه اطلاع رسانی به یک ***«یاغی و بزهکار حرفه‌ای و توانا»*** تبدیل کند.

این برنامه ***«روزنه پسین»*** نام دارد که توسط گروهی به نام ***«پرستش گاو مرده»***، به وجود آمده و امنیت نظامهای «میکروسافت» را به خطر انداخته است. در زمان حمله این ویروس، این گمان در بین متخصصان علوم رایانه‌ای قوت گرفت که گویا این گروه با شرکت متعلق به ***«بیل گیتس»*** در نبرد است و برنامه ***«روزنه پسین»*** صرفاً به رایانه‌هایی که دارای برنامه ویندوز ۹۵ و یا ویندوز ۹۸ هستند، حمله می‌کند.

نکته مهم این است که سیستم به‌کارگیری آن، بسیار ساده و آسان بوده و می‌تواند توسط هر فردی با کمترین تخصص و اطلاع، مورد استفاده قرار گیرد. یاغیهای گروه ***«پرستش گاو مرده»*** از مقر خود در ***اینترنت*** اعلام کردند که ۵۰ هزار نسخه از این برنامه خطرناک را بطور رایگان در اختیار همگان قرار داده‌اند. با قرار دادن این برنامه در رایانه، حتی ناشی‌ترین افراد می‌توانند به محرمانه‌ترین اطلاعات درون هر رایانه شخصی راه یابند و برنامه‌های موجود در آن را از بین برده و یا در آنها برنامه‌های جدیدی نصب کنند. ***«روزنه پسین»*** دارای ابعاد بسیار کوچکی بوده و می‌توان آن را در یک پیام کوتاه پنهان و سپس آن را وارد خط ***«اینترنت»*** کرد. هنگامی که دریافت کننده پیام برای خواندن محتوای پیام اقدام می‌کند، ***«روزنه پسین»*** به صورت خودکار در رایانه نصب می‌شود و تمامی اطلاعات خصوصی رایانه را برای کسی که آن را ارسال کرده است، می‌فرستد. به این ترتیب و به عقیده کارشناسان علوم رایانه‌ای از این پس هیچ اطلاعاتی، دیگر در امان نخواهد بود. در حال حاضر تهاجمهای یاغی‌ها، ۷۰ درصد از کل موارد تهاجمهای الکترونیکی را تشکیل می‌دهد.[۶]

یک آمریکایی در ایالت نیوجرسی، در غرب نیویورک، با ایجاد ویروس انفورماتیک «*ملیسا*»، به سرویسهای الکترونیک بسیاری از جمله وزارت دفاع آمریکا حمله و همگی را فلج نمود که به همین اتهام بازداشت شد. «دیوید اسمیت» ۳۰ ساله متهم است که مانع ارتباطات عمومی و دولتی شده و خسارت زیادی به سیستمهای انفورماتیک وارد کرده است. امکان دارد او به ۱۰ سال حبس و پرداخت ۴۸۰ هزار دلار جریمه محکوم شود. به گفته منابع آمریکایی، ویروس «*ملیسا*» چنان تأثیری بر روی شبکه انفورماتیک این کشور داشته است که وزارت دفاع آمریکا مجبور شد برای مدتی سیستم پست الکترونیک (E-mail) خود را ببندد. این ویروس در زمان فعال بودن خود (مارس ۹۹ میلادی) دهها شرکت بزرگ رایانه‌ای از جمله «*مایکروسافت*» و «*اینتل*» را مختل کرده است.[۷] این حکایت همچنان ادامه دارد. سیستمهای رایانه‌ای هنوز خود را کاملاً از گزند و صدمه ویروس «*ملیسا*» نرهانیده‌اند که ویروس دیگری این (بار بسیار مخرب‌تر از ویروس قبلی) به درون شبکه جهانی *اینترنت* وارد شده و از طریق پست الکترونیکی به رایانه‌ها حمله‌ور می‌گردد و موجب نابودی مدارک موجود در دیسک‌های سخت (Hard disk) رایانه‌ها می‌شود.

بنا به گزارشهای موجود در شبکه جهانی *اینترنت*، شرکتهای بزرگی مانند بوئین ای. تی. اندتی و جنرال الکتریک اعلام کرده‌اند که رایانه‌هایشان مبتلا به این ویروس شده‌اند و آنها تلاش کرده‌اند که با مسدود کردن سیستم پست الکترونیکی‌شان از شدت آسیبهای وارده به رایانه‌ها بکاهند. این ویروس به صورت یک پیام الکترونیکی به حافظه رایانه افراد وارد می‌گردد و به محض اینکه گشوده می‌شود برنامه‌های کاربردی مهمی چون «ورد اکسل و پاور پوینت» را نابود می‌کند و نامه‌های الکترونیکی شخصی را نیز از بین می‌برد. بنا به گفته و اعتقاد کارشناسان، این ویروس که به مراتب از ویروس موسوم به «*ملیسا*» نیز

خطرناک‌تر است (زیرا ملیسا توان نابود کردن کامل فایلها را نداشت)، در اسرائیل تولید شده و ظرف چند روز با سرعت در آمریکا و اروپا گسترش یافته است. این پیام الکترونیکی اینگونه آغاز می‌شود: ***«پیام الکترونیکی شما را دریافت کردم و برای شما پاسخ می‌فرستم که تا آن موقع به مدارک فشرده شده زیر توجه کنید. خداحافظ».***(۸)

در واقعه‌ای دیگر دو سوئدی به سیستم رایانه‌ای سازمان ملی فضا - هوای آمریکا (ناسا)، نیروهای مسلح این کشور (نیروهای هوایی، دریای و زمینی) و یک شرکت *اینترنت* انگلیس نفوذ کردند. این نفوذ در فاصله بین ماه اکتبر و دسامبر سال ۱۹۹۶ میلادی انجام پذیرفت و رسیدگی به جرایم آندو در ماههای پایانی سال ۱۹۹۹ صورت گرفت. دادستان سوئد معتقد است حداکثر مجازاتی که برای آنان ممکن است در نظر گرفته شود، محکومیت به دو سال زندان است.(۹)

در مورد دیگر، یک نوجوان ۱۵ ساله کانادایی، که لقب «پسر مافیایی» را بر خود نهاده بود، به همراه چند نفر دیگر به دو شبکه عمده *اینترنت* آمریکا حمله کرد. پلیس فدرال آمریکا تحقیقات خود را درباره اختلال در شبکه‌های بزرگی چون «یاهو» و «آمازون» از هنگامی شروع نمود که آنان اعلام کردند به دلیل اختلال ناشی از دریافت میلیون‌ها نامه الکترونیکی، به مدت چند ساعت فعالیتشان متوقف شده است. «پسر مافیایی» بارها تهدید کرده بود که به پایگاه *اینترنت* (C.N.N) و چند مرکز دیگر حمله رایانه‌ای خواهد کرد. به گفته کارشناسان مبارزه با حمله‌های رایانه‌ای، دانش فنی افرادی که چندین ساعت بزرگترین پایگاههای *اینترنت* آمریکا را از کار انداختند، بسیار بالا بوده است.

این حمله‌ها و ارسال و انتشار انواع ویروسها کماکان در گوشه کنار جهان ادامه دارد؛ بعضی در بردی کم و در زمانی کوتاه و بعضی در گسترهٔ جهانی و در زمانهای بسیار طولانی.

تازه‌ترین حمله‌های اینترنتی و ویروسی را هم اکنون در ماه مه سال ۲۰۰۰ میلادی (اردیبهشت سال ۱۳۷۹ هجری شمسی) شاهد هستیم. هجومی بسیار گسترده و غافلگیر کننده با خساراتی به مراتب سنگین‌تر از گذشته و این بار منطقه هجوم و حمله، رایانه‌های موجود در شرق و غرب جهان است.

و این ویروس رایانه‌ای «دوستت دارم» (I Love You)، که در همان روزهای اولیه انتشار خود میلیاردها دلار زیان مالی در سرتا سر جهان به بار آورده، نخست به سادگی در دو نشانی پست الکترونیکی در فیلیپین کاشته شد و سپس با سرعت از آنجا به دورترین نقاط جهان راه یافته است. این ویروس که هم اکنون از بیشترین سرعت انتشار در جهان برخوردار می‌باشد، روز پنجشنبه (۱۵ اردیبهشت ۱۳۷۹ برابر با ۴ مه سال ۲۰۰۰ میلادی) از فیلیپین به تایوان و از آنجا به هنگ کنگ منتقل شد و پس از آن در اروپا و سپس آمریکا وحشت آفرینی کرد. این ویروس قدرتمند تنها دو روز بعد از انتشارش در جهان، ده‌ها میلیون رایانه را آلوده ساخته و بسیاری از ساختارهای رایانه‌ای را از کار انداخته.است و میزان خسارت آن در جهان از مرز ۲ میلیارد و ۶۱۰ میلیون دلار نیز گذشته است.

این ویروس به شکل نامه‌های پست الکترونیکی با عبارت «یک نامه عاشقانه دارید»، به رایانه‌ها راه می‌یابد. گشودن نامه پست الکترونیکی آلوده به این ویروس سبب نفوذ آن به داخل ساختار رایانه و آغاز عملیات مخرب آن می‌شود. بدین گونه که خود را روی لوح فشرده رایانه دریافت کننده ذخیره کرده، وارد سیستم عامل رایانه می‌شود و بسیاری از پرونده‌ها را پاک کرد، فرمانی به ثبت می‌رساند که به موجب آن، هر بار که رایانه روشن می‌شود، این ویروس نیز آماده خرابکاری می‌گردد. هنگامی که بهره‌ور به *اینترنت* متصل می‌شود، ویروس خود را تکثیر می‌کند و یک نسخه به هر نشانی پست الکترونیکی و اتاق گپ رایانه‌ای که در «دفتر تلفن» رایانه بهره‌ور ثبت شده می‌فرستند و همه سخت افزارهای پیرامونی متصل به رایانه را شناسایی کرده و خود را به جای همه

پرونده‌های نوع موسیقی، ویدیو، عکس و برنامه‌ای نشان می‌دهد.

این ویروس همانند تبهکاران حرفه‌ای دست به تغییر چهره زده و در این مدت کوتاه به شکلهای مختلفی چون: یک لطیفه، پیامی به مناسبت روز مادر در آمریکا (۱۴ ماه مه ۲۵ اردیبهشت) و حتی هشدار به مناسبت ظهور یک ویروس جدید رایانه‌ای و نحوه مقابله با آن، درآمده است.

هم اکنون بسیاری از سایتهای رایانه‌ای در اروپا، آمریکا و دیگر کشورهای جهان، تحت شدیدترین حمله‌های اینترنتی این ویروس خطرناک قرار گرفته‌اند. تاکنون پنتاگون (وزارت دفاع)، اداره اطلاعات مرکزی (C.I.A) و پلیس فدرال آمریکا (F.B.I) به صورت محسوسی مورد هجوم ویروس مذکور قرار گرفته است. رد پای این ویروس در هند نیز از سوی متخصصان علوم رایانه شناسایی شد. به گزارش روزنامه انگلیسی زبان «هندوستان تایمز»، خبر پخش این ویروس در دهلی نو اولین بار توسط یک شرکت هندی، که با اوراق بهادار سر و کار دارد، گزارش شد.(۱۰)

از سوی دیگر، از میان کشورهای منطقه خلیج فارس، اولین گزارش اعلام خطر و هشدار، از سوی کارشناسان رایانه در کویت با مضمون ***«برای مصون ماندن دستگاههای رایانه‌ای از خطر حمله ویروس جدید از خواندن پست‌های الکترونیکی ناشناس، یا عبارت «دوستت دارم» یا «دوستت دارم ۲۰۰۰» خودداری کنند»***، به کاربران شبکه اینترنت ارائه شد. هر چند آمار رسمی و دقیقی از تعداد دستگاههای آسیب دیده در بخشهای مختلف کویت اعلام نشده، ولی کاربری فراوان *اینترنت* در این کشور، احتمال وسیع بودن آسیب دیدگی رایانه‌های خصوصی افراد و شرکتها را مطرح کرده است.

«تروور مالار» قائم مقام وزیر ارتباطات زلاندنو نیز گفت: ***«انتشار این ویروس، شدیدترین بلای رایانه‌ای است که بر سر کشورش آمده است».***

همچنین «دمیتری چیچوگف»، رئیس اداره مبارزه با تبهکاریهای رایانه‌ای در وزارت کشور روسیه، دو روز پس از انتشار جهانی ویروس اعلام کرد:

«ویروس رایانه‌ای مذکور نتوانسته است صدمه چندانی به سیستم‌های رایانه‌ای این کشور برساند».

هم اکنون همه نگاهها به فیلیپین و مانیل به عنوان مرکز این حمله اینترنتی و بزهکاری رایانه‌ای دوخته شده است. پلیس فدرال آمریکا و پلیس بین‌المللی (اینترپول)، این ویروس را تا فیلیپین ردگیری کرده و متوجه شده‌اند که مظنون یک جوان ۲۳ ساله است که در ناحیه متوسط‌نشین مانیل، پایتخت فیلیپین، سکونت دارد؛ اما این احتمال را نیز می‌دهند که شاید این ویروس از شهر و یا کشور دیگر وارد شبکه شده باشد.

از طرفی پلیس فیلیپین نیز اعلام کرده است که به طراح ویروس رایانه‌ای (دوستت دارم) نزدیک شده است. در این میان ارائه کنندگان نرم افزارهای ضد ویروس برای مقابله با ویروس مذکور، تدابیر گسترده‌ای را اتخاذ کرده‌اند و ضمن درخواست از مشترکان خود برای به روزکردن نرم افزارهای خریداری شده از آنان خواسته‌اند که تازه‌ترین پرونده‌های خود را از «**اینترنت**» تهیه کنند.

آیا دستیابی به امنیت در اینترنت ممکن است؟

معروفترین مهاجم رایانه‌ای آمریکا که اخیراً از زندان آزاد شده و حالا هم بیکار است، در پاسخ به این سؤال می‌گوید: «امنیت رایانه مثل قفل زدن به در می‌ماند. اگر کسی واقعاً بخواهد داخل شود، می‌تواند این کار را از پنجره انجام دهد».

او که یک جوان ۳۶ ساله به نام «کوین میتینگ» است و دیگر حق ندارد به

هیچ کاری که از دور و نزدیک با رایانه سر و کار داشته باشد، مشغول شود، این حرفها را در کنگره آمریکا و در برابر سناتورها که او را دعوت کرده بودند، گفته است. همچنین او در توضیحات خود به سناتورهای آمریکایی می‌گوید که در تمام مدتی که مهاجم انفورماتیک بوده موفق شده است به همه سیستمهایی که هدف گرفته بود نفوذ کند، بجز یک سیستم، که آن هم تحت نفوذ مهاجم دیگری در انگلیس قرار داشت. وی در ادامه مطالب خویش اظهار می‌دارد: ***«در بسیاری از موارد نیازی به حملات فنّی نداشته است، زیرا با حرف کشیدن از کارکنان شرکتهای بزرگی مثل «موتورولا» و «نوکیا» به راحتی اطلاعات کلیدی و رمزها را به دست آورده است».***

بر این اساس جهت برقراری امنیت در *اینترنت* نه تنها باید چاره‌ای برای حملات فنّی و انفورماتیکی (که هر روز پیچیده‌تر می‌شود) اندیشید، بلکه باید نسبت به آموزش کارکنان و کاربران رایانه‌های دولتی و خصوصی اقدام شایسته صورت گیرد.

در همین راستا و در جهت سنجش میزان ایمنی شبکه‌های اطلاع رسانی و رایانه‌ای یک نمایشگاه فن‌آوری اطلاعاتی در سنگاپور اعلام کرده است: به هر کسی که بتواند به سایتهای این نمایشگاه در *اینترنت* دستبرد بزند، ۱۰ هزار دلار جایزه می‌دهد. مسؤولان این نمایشگاه می‌گویند: ***«در واقع پس از حمله رایانه‌ای اخیر، ویروسهایی همانند «ملیسا»، «چرنوبیل» و... به این فکر افتادند سایتی برای راهزنان رایانه‌ای در اینترنت ایجاد کنند و ضمن اعطای جایزه نقاط ضعف و کور سیستم ایمنی رایانه‌ها را شناسایی و نسبت به بستن آن اقدام نمایند.»***

همچنین، مزاحمان پاک نیتی به نام هکرها (Hackers) هم وجود دارند. آنان (متخصصان رایانه و سیستمهای اطلاعاتی هستند که به سیستمهای پیشرفته و سایتهای بزرگ نفوذ کرده و کار آنها را مختل می‌نمایند. آنها

عقیده دارند فعالیت آنها با حسن نیت همراه بوده و در حقیقت با این اقدام سریع باعث شناسایی و رفع نقایص سیستمهای اطلاعاتی می‌شوند.

کارشناسان علوم رایانه‌ای، اختلال در سایتهای بزرگی چون «Ebay» و «Yahoo» را به این گروه نسبت می‌دهند به همین خاطر، بودجه مخصوصی از سوی دولت آمریکا به F.B.I اختصاص یافته تا جلوی مزاحمت این گروه پاک نیت گرفته شود.

گفتنی است حملات اینترنتی همیشه از طریق ارسال و انتشار ویروس صورت نمی‌گیرد، بلکه در بسیاری از موارد از راه نفوذ در سیستمهای اطلاعاتی و دستکاری در آن به گونه‌های مختلف انجام می‌پذیرد.

در شهریور ماه سال ۷۸ یک مهاجم اینترنتی در گوشه نامعلومی از جهان در هنگامی که احزاب سیاسی استرالیا سرگرم مبارزات انتخاباتی بودند، وارد «وب سایت» حزب حاکم لیبرال استرالیا شد و ضمن ایجاد تغییرات در محتوا، مطالب آن را به صورت مضحکی درآورد و در پایان چند عکس مستهجن نیز ضمیمه آن کرد. این عمل مهاجم ناشناس لطمه شدیدی به حیثیت حزب لیبرال وارد ساخته بود.(۱۱)

همچنین در مورد دیگری مهاجم یا مهاجمان ناشناس ورود به سیستم رایانه‌ای دانشگاه استانفورد آمریکا، رمز پست الکترونیکی ۴۵۰۰ نفر از دانشجویان و استادان را مورد دستبرد قرار دادند. مهاجمان برای سه هفته، بدون اینکه کسی متوجه شود، به مطالب پستهای الکترونیکی این دانشگاه دسترسی داشته‌اند.(۱۲)

نقض حقوق نویسندگان، هنرمندان و ناشران

گردش و سیر پیامها و اطلاعات بدون اجازه اولیه، از جمله موارد نقض حقوق اولیه افراد بوده و حق حاکمیت افراد را نیز از بین می‌برد.

بـزرگراهـهای اطـلاعاتی، قـوانین و حـقوق نـاشران، مـصنفان و هـنرمندان و مـالکان آثـار عـلمی و تـاریخی را تـغییر داده است؛ چـرا کـه نـه تـنها آثـار آنـان و از طـریق شـبکه‌های فـضایی الکـترونیکی جـمع‌آوری و تـقسیم و تـوزیع مـی‌شود، بـلکه بـانکهای اطـلاعاتی بـا دسـترسی بـه اطـلاعات موجود، مـحصولات مـختلفی را تـهیه و بـه مشـتریان جـهانی ارائـه مـی‌کنند که خـارج از حـدود کـنترل عـهدنامه‌ها و مـقررات مـربوط بـه حـق چـاپ و تـوزیع دهـه‌های قـبلی مـی‌باشد و بـه هـمین خـاطر مسـائل مـربوط بـه آن از جـمله مـوضوعات مـورد اخـتلاف مـلل و دولتها تـهیه شـده کـه یکـی از مشکلات و معماهای بزرگ حقوقی و تجارتی سازمان تجارت بین‌الملل (گات) می‌باشد.

نقض حاکمیت ملی

انـتقال تـصاویر و اطـلاعات از طـریق شـبکه‌های اطـلاع رسـانی مـرز جغرافیایی نمی‌شناسد. بر این اساس، بطور آشکار حاکمیت ملی کشورهایی که خواهان بعضی از مطالب ارسالی نیستند، نقض می‌شود. به عنوان مثال، انتقال تصاویر و اطلاعات غیر قانونی فرامرزی همچنان از مشکلات لاینحل *اینترنت* باقی مانده است. انتشار برخی اطلاعات و تصاویر، مـمکن است در کشـوری غیرقانونی محسوب شود؛ ولی درکشور دیگر قانونی باشد. در این صورت حتی اگر ناشر آن نیز مشخص شود، امکان تعقیب قانونی وی در فراسـوی مـرزها، بدون موافقت مراجع قانونی کشور محل اقامت ناشر وجود ندارد.

فن‌آوری رایانه و تجاوز به قلمرو خصوصی افراد

«حریم شخصی» به عنوان یک ارزش اجتماعی و حـق قـانونی، طـیف گسترده‌ای از حقوق مربوط به استقلال شخصی را، که به عنوان «حق به حال

خود گذاشته شدن» یا «عدم مداخله در امور خصوصی دیگران» شناخته شده است، شامل می‌شود. از جهت وجود متغیر ارتباط بین افراد، حریم شخصی حق اعمال کنترل بر اطلاعات درباره شخص نیز معنی می‌دهد. این اصول، تاریخی طولانی دارند و در شرایطی که فن آوریهای جدید تهدیدهای روزافزون برای حریم فردی به وجود می‌آورند، به رشد و تکامل خود ادامه داده‌اند. از اواسط دهه ۱۹۷۰ موضوع حمایت از اطلاعات خصوصی، بر محور رشد انفجاری رایانه و توانایی آن برای جمع آوری، جست و جو، مقایسه و ادغام اطلاعات خصوصی درباره افراد می‌چرخید. بدین ترتیب تهدید جدی برای حریم خصوصی افراد در عصر ارتباطات پدید آمده است.(۱۳)

امروزه اهمیت حمایت از زندگی افراد در مقابل خطرهای ناشی از فن‌آوری رایانه‌ای و انفورماتیک، از دغدغه‌های مهم مربوط به شبکه‌های اطلاع رسانی جهانی است. رایانه‌های بزرگ امروزی که در اختیار شبکه‌های اطلاعاتی قرار دارند، خصوصی‌ترین و شخصی‌ترین اطلاعات مربوط به افراد را جمع آوری می‌کنند و به عبارتی تقریباً همه افراد پرونده‌دار شده‌اند؛ بدون آنکه از محتوای پرونده خود باخبر باشند. در این صورت، افراد بداندیش با دستیابی به اطلاعات شخصی، سوء استفاده‌های گوناگونی را مرتکب می‌شوند و این به مدد توانایی این شبکه‌ها که همانند شمشیر دو لبه عمل می‌کنند، می‌باشد.

چند سال پیش و بعد از مرگ فرانسوامیتران، رئیس جمهور سابق فرانسه هنگامی که پزشک معالج او، اسراری از بیماری و زندگی او را در کتابی فاش کرد، به درخواست خانواده او و همچنین نظام پزشکی فرانسه، فروش کتاب از طرف دولت ممنوع شد. اما چند ساعت بعد تعدادی مهندس رایانه در گرونوبل (Grenoble) تمام کتاب را روی شبکه *اینترنت* وارد کرده و در دسترس کنجکاوان قرار دادند.(۱۴)

قتل از طریق رایانه‌های متصل به شبکه‌های اطلاع رسانی

قتل و آدم‌کشی از طریق یک رایانه متصل به شبکه «*اینترنت*» چیزی است که هنوز بیشتر به داستانهای علمی ـ تخیلی می‌ماند؛ ولی می‌تواند به عنوان یک ابزار در این جهت به کار رود. پلیس ایالت پنسیلوانیا در آمریکا اخیراً کشف کرده است که در یک مورد گروگانگیری و قتل، شخصی که اکنون متهم به قتل می‌باشد، قبلاً از طریق «*اینترنت*» با قربانی خود ارتباط برقرار کرده بوده است. حتی بیل کلینتون، رئیس جمهوری آمریکا نیز در صندوق پست الکترونیکی خود پیامهایی را از افراد ناشناسی دریافت کرده بود که او را تهدید به قتل کرده‌اند.(۱۵)

اخیراً یک جوان ۲۲ ساله دانمارکی طی ۷۹ نامه الکترونیکی، یکی از روزنامه‌نگاران روزنامه‌های پرتیراژ دانمارک و خانواده او را به خاطر نوشتن مقاله در مورد یک درگیری، که به چاقوکشی انجامیده بود و پای او را به میان می‌کشید، به مرگ تهدید کرد. با این که نامه‌های مزبور از راه نشانیهایی در آمریکا ارسال شده بود تا هویت نویسنده آن فاش نشود، پلیس توانست رد نویسنده نامه‌ها را پیدا و او را بازداشت کند که در نهایت به پرداخت ۲۰۰ کرون (۲۹۴ دلار) جریمه محکوم شد.(۱۶)

ایجاد خبرنامه‌های اختصاصی جنایتکاران، بزهکاران و نژادپرستان

هم اینک با گشت و گذاری کوتاه مدت در جهان مجازی *اینترنت* می‌توان به خبرنامه‌های اختصاصی مربوط به بعضی از گروههای بزهکاران دست یافت. همجنس بازان به راحتی خبرنامه اختصاصی تشکیل داده و اقدام به عضوگیری و ارتباط با اعضای خود می‌کنند و پیوسته اخبار و اطلاعات مربوط به گروه خود را به اطلاع اعضای خود رسانده و بدین وسیله امکان ایجاد یک حرکت جهانی را در راستای اهداف نامیمون خود، فراهم می‌کنند.

گانگسترها به راحتی با هم در پوشش عناوین جعلی ارتباط برقرارکرده و به تبادل تجربه می‌پردازند و احیاناً از خطرات موجود همدیگر را باخبر می‌سازند. رؤسای شبکه‌های توزیع مواد مخدر، فروشندگان سلاح و دیگر سازمانهای مافیایی و جنایتکاران بدون هیچگونه نگرانی اقدام به تشکیل جلسات شور و مشورت و روابط کاری می‌کنند.

از سوی دیگر، نژادپرستان اعم از نئونازیهای آلمان، ملی‌گرایان آمریکایی، سر تراشیده‌های نژادپرست انگلیسی و دیگر گروههای نژادپرست، در سراسر جهان به تبلیغات نژاد پرستانه پرداخته و با استفاده از شعارهای رایانه‌ای اعضای خود را به اقدامات آشوبگرانه و خشونت زا تحریک می‌کنند. خطابه‌های مملو از خشم و نفرت آنان، از یک رایانه به رایانه دیگر منتقل می‌شود و گروههای افراطی نژاد پرست در سراسر جهان به ارتباط نزدیک با یکدیگر می‌پردازند.

گفتنی است تعداد سایتهای دست راستی‌های افراطی آلمان در *اینترنت* به شدت افزایش پیدا کرده و اکنون به صدها سایت رسیده است؛ در حالی که این افراد در سال ۱۹۹۶، فقط ۳۰ سایت داشته‌اند. به این تعداد باید صدها سایت موجود در اروپا و آمریکا افزوده شود. به نوشته روزنامه «فرانکفورت‌تر آلگمانیه زونتاگ سایتونگ» به نقل از سرویس اطلاعاتی داخلی آلمان، شبکه *اینترنت* عملاً یک فضای فاقد کنترل قضایی برای دست راستی‌های افراطی به شمار می‌رود و این افراد فقط به تبلیغات در این شبکه اکتفا نمی‌کنند، بلکه توصیه‌های عملی خود را برای ساخت مواد منفجره نیز از همین طریق ارائه می‌دهند.

آموزش جرایم از طریق شبکه‌های اطلاع رسانی

گفته شد محتویات نامطلوب شبکه‌های اطلاعاتی بدون کمترین مانعی

به کودکان و نوجوانان ارائه می‌شود. این شبکه‌ها به مثابه جهان واقعی عمل می‌کنند و در تاروپود آن می‌توان خوب و بد را مشاهده کرد.

بعضی از اطلاعات موجود در شبکه‌های اطلاعاتی ـ که کم هم نیستند ـ چگونگی ساخت مواد ترکیبی مواد مخدر با استفاده از مواد و داروهایی که در دسترس همگان قرار دارد، به رایگان آموزش می‌دهد. بر این اساس و طبق دستورالعمل، هر کودک و نوجوانی به راحتی امکان دستیابی به مواد مخدر خطرناک را خواهد داشت. همچنین انواع خاصی از اخبار و اطلاعات وجود دارد که محلهای تهیه مواد مخدر را معرفی می‌کند. البته پیامهای هشدار دهنده از سوی پدر و مادرها نیز در این باره به چشم می‌خورد. همچنین در برخی موارد اثرات جنبی و خطرناک استعمال مواد مخدر نیز ذکر شده است.

چگونگی ساخت بمب و مواد منفجره با ضریب تخریب بالا، از دیگر اطلاعات موجود در شبکه‌هاست. در نشریه «ال پائیس» آمده بود: یک نوجوان توانسته است با استفاده از اطلاعات کسب شده از شبکه ***اینترنت*** بمب ناپالم بسازد.(۱۷)

در واقعهٔ دیگری پلیس آمریکا اقدام به دستگیری دانش آموزانی کرد که با اطلاعات موجود در شبکه ***اینترنت***، بمب ساخته بودند و قصد انفجار مدرسهٔ خود را داشتند.

انفجار ۱۹ آوریل اوکلاهما، که به بهای جان بیش از ۱۶۰ نفر انجامید، واحدهای پلیس مسؤول جرایم رایانه‌ای را در حالت آماده باش قرار داد؛ زیرا مجرمان، بزرگراههای اطلاعاتی را نیز مورد استفاده قرار داده بودند. همچنین در ***اینترنت*** متنی یافت شد که نویسنده آن به توضیح چگونگی ساخت بمب ـ از همان نوعی که در انفجار اوکلاهما به کار رفت ـ پرداخته بود.(۱۸)

همچنین در حادثه دیگری دو پسربچه استرالیایی، که از طریق ***اینترنت*** چگونگی ساخت بمب را یاد گرفته بودند، هنگام درست کردن بمب دراثر

انفجار آن، به شدن مجروح شدند. گفتنی است دسترسی به ***اینترنت*** در استرالیا برای بسیاری از کودکان خیلی ساده می‌باشد و بسیاری از خانه‌ها و مدارس به ***اینترنت*** وصل هستند.

در تازه‌ترین اقدام از این دست و از سوی دانش‌آموزان استرالیایی، هشت پسر و دختر کلاس ششم و هفتم دبستان در ونکووریک پایگاه ***اینترنت*** برقرار کرده بودند که در ابتدا برای تشویق دانش‌آموزان در بازیهای مدرسه به کار می‌رفت. این اقدام اگر چه در ابتدا بی‌ضرر بود، اما پس از مدتی والدین دانش‌آموزان گزارش دادند که این پایگاه به مرکزی خطرناک در ترویج نژادپرستی، حماقت، نفرت و مسائل جنسی تبدیل گردیده است و سایر دانش‌آموزان مدرسه هدف این امور قرار گرفته‌اند.

دانش‌آموزان این مدرسه نه تنها قربانی این مسائل نفرتی قرار گرفته بودند، بلکه نام واقعی آنان نیز در پایگاه ***اینترنت*** درج شده و از همین رو به راحتی می‌توانستند توسط افراد خلافکار شناسایی و مورد سوء استفاده قرار گیرند.

بطور کلی در مدارس آمریکای شمالی، پایگاه ***اینترنت*** مجانی توسط دانش‌آموزان دبیرستان طراحی و مورد استفاده فراوانی قرار می‌گیرد که زمینه‌های مثبت و منفی بسیاری را شامل می‌گردد. با این حال، این اولین بار بود که در یک مدرسه ابتدایی نیز چنین پایگاهی مورد سوءاستفاده و وسیله اقدامات بزهکارانه قرار می‌گرفت.

آنچه که در این میان و برای همگان آزاردهنده است، تمایل کودکان کم سن و سال به استفاده‌های آزار دهنده از ***اینترنت*** می‌باشد. به هر حال این اتفاقات به خوبی نقش غیر قابل انکار فن آوری پیشرفته را در تسهیل بزهکاری نشان می‌دهد. به گونه‌ای که به مدد قدرت فن آوری امروزی خصوصاً فن آوری رایانه‌ای و اینترنتی، کودکان خردسال نیز به صف بزهکاران حرفه‌ای پیوسته‌اند.

عدم حاکمیت قانون بر شبکه

یکی از معایب شبکه‌های اطلاع رسانی جهانی، عدم حاکمیت قانون بر آن می‌باشد و پرواضح است که عدم حاکمیت قانون در هر مجموعه‌ای موجب هرج و مرج خواهد شد. به همین خاطر، نقل و انتقال پیامها روی شبکه، مطمئن و ایمن نبوده و راه را برای سوء استفاده باز می‌کند و افراد بداندیش، بزهکاران باسابقه و...از *اینترنت* مانند ابزاری به منظور انجام کارهای خلاف خود استفاده می‌کنند. در حقیقت قواعد حقوقی موجود در جهان بـه هـم ریـخته و از ایـن رهگذر آسیبهای جدید اجتماعی پدیدار شده است.

عدم وجود مدیریت و کنترل روی شبکه

یکی دیگر از معایب شبکه این است کـه هـیچ مأمـور، سـرپرست و یـا دستیاری در راه عبور مطالب تدوینی و تصویری ایـن شـبکه‌ها در سـطح بـین المللی وجود ندارد و در حقیقت هیچ کس مالک *اینترنت* نیست.

در *اینترنت* کسی قدرت اخراج دیگری را ندارد و در «کلید کنترل مرکزی» موجود نیست تا در مواقع لزوم، اقدام به از کار انداختن کل شبکه نمود؛ زیـرا طراحی اولیه *اینترنت* به گونه‌ای بوده است که در صورت از کار افتادن بخشی از شبکه، سایر بخشها بتوانند به کار خود ادامه دهند؛ به بیان دیگر، «تمرکز زدایی» از اصول اولیه پایه گذاری *اینترنت* بوده است.

در مورد مدیریت و هدایت *اینترنت* می توان به وجود گروههای داوطلب در این زمینه اشاره کرد. به عنوان نمونه بالاترین مرجعی که تحولات *اینترنت* را رهبری می‌کند، به اختصار (I.S.O.C) (Internet Society) نامیده مـی‌شود. ایـن سازمان متشکل از اعضای داوطلب است که هدف آن، توسعه فن‌آوری موجود در جهت گسترش تبادل اطلاعات ذکر شـده است. "I.S.O.C" دارای شـورایـی متشکل از کارشناسان عالی‌رتبه است که مسؤولیت فنی تحولات *اینترنت* را بر

عهده دارد و آن را به اختصار "L.A.B" (Internet Architecture Board) یا «هیأت عالی معماری *اینترنت*» می‌نامند. این هیأت دارای جلسه‌های مستمری است که استانداردهای جدید در آن تصویب می‌گردد؛ منابع مالی به فعالیتهای مختلف تخصیص داده می‌شود و تصمیمهای جدید را در مورد امور شبکه اعلام می‌نماید. هیأت دیگری در درون *اینترنت*، از اعضای داوطلب تشکیل شده است که به اختصار "L.E.T.F" (Internet Engineeing Task Force) یا «گروه مهندسی *اینترنت*» نامیده می‌شود و دارای جلسه‌های مستمری است که در آن مسائل کوتاه مدت همچون انتشار گزارشها و مدارک، پذیرش و افکار تازه که از سوی داوطلبان عرضه شود، مورد بررسی قرار می‌گیرد.(۱۹)

فروش نوزادان از طریق اینترنت

جهان امروز ویژگیهای خاص خود را دارد و کاملاً متفاوت با گذشته عمل می‌کند. نوع علایق و سلایق مردمان روز به روز متنوع و اعجاب‌انگیز می‌شود و در این میان سودجویان نیز بسته به علایق و سلایقشان تمام همت خود را جهت بهره‌برداری هر چه بیشتر مصروف می‌دارند. امروزه خرید و فروش فرزندان از سوی والدین به صورت امر طبیعی در آمده است. پدر و مادری که در مقابل مقادیری پول فرزند خود را می‌فروشند و زن و شوهری که به هر دلیلی فرزند ندارند، و ضمن نثار پول بدین صورت صاحب فرزند می‌شوند. اینان بسته به علاقه و میل خود از بین کودکان فراوان آماده فروش یکی را انتخاب و با خود می‌برند. درست مانند قرنهای ۱۷ و ۱۸ و حتی ۱۹ میلادی در اروپا، که در آن، سیاهان آفریقایی و بومیان قاره‌های دیگر به مدد آتش توپ، تفنگ و کشتیهای جنگی به اسارت و بردگی اربابان سفیدپوست اروپایی در می‌آمدند و سفید پوستان ضمن بیگاری کشیدن از آنها، هر زمان که می‌خواستند نسبت به نابودیشان اقدام می‌کردند.

این تجارت کم و بیش در گوشه و کنار جهان در حال وقوع می‌باشد، ولی در ایتالیا به صورت یک تجارت پر سود وکم زحمت (البته کمی متفاوت با بخشهای دیگر جهان) درآمده است. در ایتالیا این تجارت حتی نوزادانی که هنوز به دنیا نیامده‌اند را نیز در برمی‌گیرد. بر اساس بعضی از گزارشها، در حال حاضر با پرداخت ۲۰ میلیون لیر (تقریباً ۱۱ هزار دلار) می‌توان یک نوزاد از طریق *اینترنت* خریداری کرد. مدیریت این طرح که خدمات آن از طریق *اینترنت* صورت می‌گیرد، بر عهده یک رومانیایی الاصل مقیم آمریکا صورت می‌گیرد. این شخص سودجو از وضعیت بحرانی میلیونها زوج بی فرزند سوء استفاده کرده و یک سازمان تهیه و تحویل نوزاد در سطح بین المللی به راه انداخته است. ممکن است سؤال شود که نوزادان متولد نشده چگونه به خریداران معرفی می‌شوند و خریداران با چه مشخصات مشتاق خرید آنها می‌شوند. باید گفت مغز متفکر این تجارت شیطانی برای این مشکل نیز چاره‌ای اندیشیده است این شبکه به جای فرستادن عکس نوزادان به پیش فروش کودکانی که هنوز به دنیا نیامده‌اند، می‌پردازند؛ بدین ترتیب که عکس مادرهای جوان اهل رومانی به همراه مشخصات، گواهی سلامت و معاینات پزشکی آنها از طریق شبکه *اینترنت* در اختیار زوجهایی که خواهان خرید نوزاد هستند، گذاشته می‌شود. پس از عقد قرارداد، پرداختها به صورت قسطهای متعدد صورت می‌گیرد و در پایان مادر برای زایمان به ایتالیا سفر می‌کند؛ زیرا طبق قانون و براساس سیستم خاک در اعطای تابعیت، هر نوزادی که در این کشور به دنیا بیاید، شهروند ایتالیایی است. پس از زایمان نیز همه کارها از طریق قانونی و البته توسط وکیلان زبردست و آشنای به قوانین انجام می‌شود. هم اکنون مقامات قضایی ایتالیا تحقیقات گسترده‌ای را درباره فروش نوزادان از طریق *اینترنت* آغاز کردند که تا دستیابی به هر گونه نتیجه و متعاقب آن پیش‌بینی ضمانت‌های اجرایی قانونی در جهت مقابله با این امر، در سراسر قاره اروپا شبکه‌های مخفی خرید و فروش نوزادان همچون اختاپوسی ریشه دوانیده و مبارزه با آن را مشکل کرده است. ◄►

پانویس

۱- موحد،سیمین: انقلاب دوم اینترنت،به‌نقل از هفته نامه «گاردین» ۲ نوامبر ۹۷ شماره ۱۸.

۲-«طرف تاریک اینترنت»، کامپیو۱۶ - چاپ اسپانیا به نقل از رسانه، سال ششم، شماره ۴،ص ۵۵.

۳- اردبیلی، محمد علی و نجفعلی ابرندآبادی، علی حسین: گزارش گروه ۲ از پانزدهمین کنگره بین المللی حقوق جزا (جرایم انفورماتیک و رایانه‌ای و سایر جرایم در قلمرو تکنولوژی انفورماتیک)، مجله تحقیقات حقوقی، شماره ۱۷-۱۶ ص ۴۵۷.

۴- همان، ص ۴۵۵ و ۴۵۴.

۵- بوسا، آندرو، بزهکاری بین المللی، ص ۵۸.

۶- جمهوری اسلامی، ۷۷/۶/۱۵، ص ۵.

۷- کیهان، ۷۸/۱/۱۷، ص ۱۵.

۸- جمهوری اسلامی، ۷۸/۳/۲۵، ص ۵.

۹- اطلاعات (ضمیمه)، ۷۸/۶/۷، ص ۸.

۱۰- جمهوری اسلامی، ۷۹/۲/۱۸، ص ۵.

۱۱- ایران، ۷۸/۶/۱۷، ص ۱۲.

۱۲- همان، ۷۷/۸/۲۲، ص ۵.

۱۳- دایرةالمعارف بین‌المللی ارتباطات، ترجمه علی کسمایی، رسانه، سال هفتم، شماره چهارم ص ۳۳.

۱۴- غفاری، ستاره: رسانه‌های نوین در خدمت تساوی جهانی یا تشدید کننده نابرابری‌ها، رسانه، سال هفتم، شماره اول، ص ۲۱.

۱۵- طرف تاریک اینترنت، مترجم، وظیفه‌شناس، رسانه، سال ششم، شماره چهارم، ص ۵۴.

۱۶- کیهان، ۷۷/۶/۷، ص ۱۵.

۱۷- هفته نامه صبح، شماره ۱۹، ص ۲۰.

۱۸- طرف تاریک اینترنت، رسانه، سال ششم، شماره چهارم، ص ۵۴.

۱۹- محسنی، منوچهر: شبکه اطلاعاتی اینترنت، ویژگی‌ها و تأثیرات اجتماعی - فرهنگی، رسانه، سال هفتم، شماره اول، ص ۲۵.